CONSENSYS
Diligence

Blank Art (Wrapped Cryptopunks) Spot-Check

October 1st, 2020
Shayan Eskandari

Project Details

Code: https://etherscan.io/address/0xb7f7f6c52f2e2fdb1963eab30438024864c313f6#code

Project details:

- https://wrappedpunks.com/
- Wrapper on Cryptopunks to ERC721
  - "Wrapped Cryptopunks", "WPUNKS"
- Second Rank on OpenSea

Goals

- As the project is getting traction, the dev team would like to review the code to make sure there are no security issues
- After the review, if nothing is found, the dev team would like to renounce the ownership of the contract
- Any attack surface, can anything put the PUNKs at risk.
  - Approval
  - Transfer
  - Does the proxy work as intended?
- Verify OZ implementations

Review

General

- The code is not complex, and uses many of the open source code for its core functionality (See Observations)
- No documentation is available for the codebase other than inline comments
- No test suite is available at the time of the spot check

Observations

- The main *ERC721* functionality is using OpenZeppelin implementation (7d7cbcad):
  - Pausable
  - SafeMath
  - Strings
  - ERC721
    - ERC721Enumerable
    - ERC721Metadata
    - ERC721Full
  - ERC165
  - Ownable
  - Interfaces

- It should be enforced to prevent token transfer to the *WrappedPunk* contract itself. As the contract is live on the mainnet, it can only be done through the user interface (UI).
- *TransferFrom* does proper checks for ownership and approval before finalizing the transfer
- Proper checks in *registerProxy()* prevents in-transfer tokens getting stuck on the proxy address (enforcing one proxy per address)

Owner Capabilities

- Set BaseURI
  - In case owner is renounced, the *BaseURI* can not be changed on the contract (current URI: https://wrappedpunks.com:3000/api/punks/metadata/)

- Pause & Unpause the contract. Which pauses the following functionalities:
  - Mint
  - Burn
  - TransferFrom

- Ownership
  - Transfer Ownership
  - Renounce Ownership (*owner = address(0)*)

UserProxy Contract

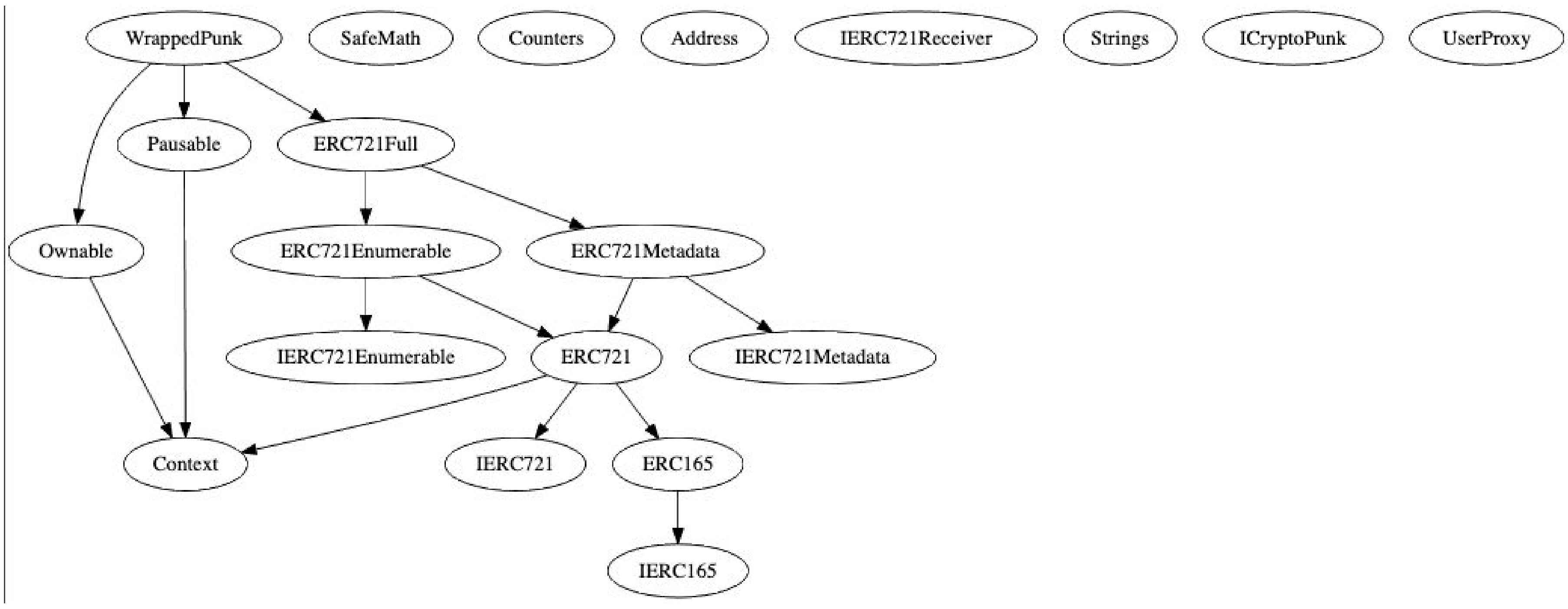
- On *transfer,* the contract expects *punkContract* to return a boolean, however the implementation of *punkContract.transferPunk()* does not return any value. As *transferPunk()* either throws an exception or runs successfully, this is not an issue.

- Owner of each *UserProxy* is the *WrappedPunk* contract, this handles the token transfers properly

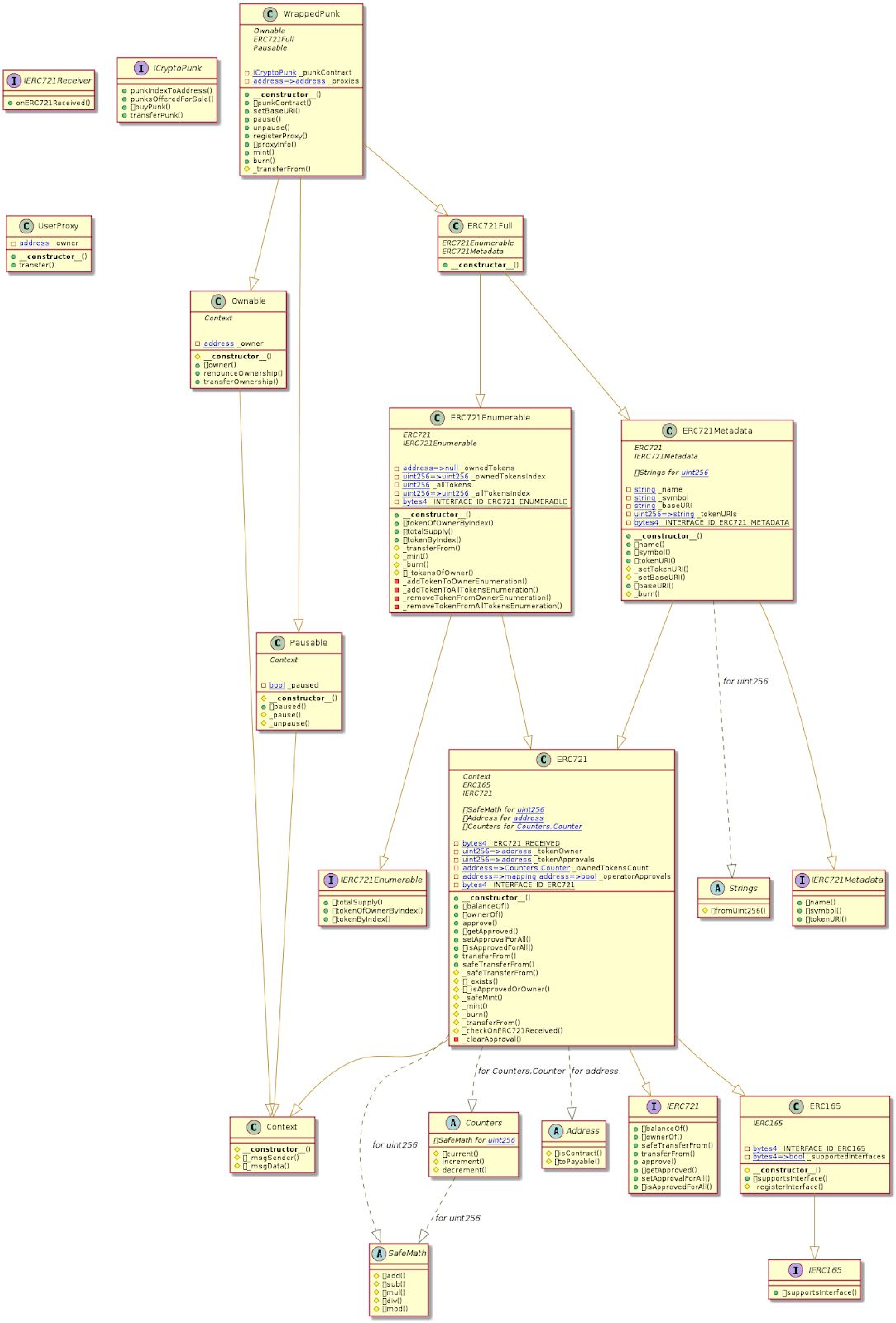
---

Analysis Graphs

Inheritance



UML


IERC721Receiver
onERC721Received()
ICryptoPunk
punkIndexToAddress()
punksOfferedForSale()
buyPunk()
transferPunk()
WrappedPunk
Ownable
ERC721Full
Pausable
ICryptoPunk _punkContract
address=>address _proxies
__constructor__()
punkContract()
setBaseURI()
pause()
unpause()
registerProxy()
proxyInfo()
mint()
burn()
_transferFrom()
UserProxy
address _owner
__constructor__()
transfer()
ERC721Full
ERC721Enumerable
ERC721Metadata
__constructor__()
Ownable
Context
address _owner
__constructor__()
owner()
renounceOwnership()
transferOwnership()
ERC721Enumerable
ERC721
IERC721Enumerable
address=>null _ownedTokens
uint256=>uint256 _ownedTokensIndex
uint256 _allTokens
uint256=>uint256 _allTokensIndex
bytes4 _INTERFACE_ID_ERC721_ENUMERABLE
__constructor__()
tokenOfOwnerByIndex()
totalSupply()
tokenByIndex()
_transferFrom()
_mint()
_burn()
_tokensOfOwner()
_addTokenToOwnerEnumeration()
_addTokenToAllTokensEnumeration()
_removeTokenFromOwnerEnumeration()
_removeTokenFromAllTokensEnumeration()
ERC721Metadata
ERC721
IERC721Metadata
Strings for uint256
string _name
string _symbol
string _baseURI
uint256=>string _tokenURIs
bytes4 _INTERFACE_ID_ERC721_METADATA
__constructor__()
name()
symbol()
tokenURI()
_setTokenURI()
_setBaseURI()
baseURI()
_burn()
Pausable
Context
bool _paused
__constructor__()
paused()
_pause()
_unpause()
for uint256
ERC721
Context
ERC165
IERC721
SafeMath for uint256
Address for address
Counters for Counters.Counter
bytes4 _ERC721_RECEIVED
uint256=>address _tokenOwner
uint256=>address _tokenApprovals
address=>Counters.Counter _ownedTokensCount
address=>mapping address=>bool _operatorApprovals
bytes4 _INTERFACE_ID_ERC721
__constructor__()
balanceOf()
ownerOf()
approve()
getApproved()
setApprovalForAll()
isApprovedForAll()
transferFrom()
safeTransferFrom()
_safeTransferFrom()
_exists()
_isApprovedOrOwner()
_safeMint()
_mint()
_burn()
_transferFrom()
_checkOnERC721Received()
_clearApproval()
IERC721Enumerable
totalSupply()
tokenOfOwnerByIndex()
tokenByIndex()
Strings
fromUint256()
IERC721Metadata
name()
symbol()
tokenURI()
for Counters.Counter
for address
Context
__constructor__()
_msgSender()
_msgData()
for uint256
Counters
SafeMath for uint256
current()
increment()
decrement()
Address
isContract()
toPayable()
IERC721
balanceOf()
ownerOf()
safeTransferFrom()
transferFrom()
approve()
getApproved()
setApprovalForAll()
isApprovedForAll()
ERC165
IERC165
bytes4 _INTERFACE_ID_ERC165
bytes4=>bool _supportedInterfaces
__constructor__()
supportsInterface()
_registerInterface()
for uint256
SafeMath
add()
sub()
mul()
div()
mod()
IERC165
supportsInterface()